Journal of Number Theory **79**, 19–28 (1999)
Article ID jnth.1999.2418, available online at http://www.idealibrary.com on IDEAL®

Deformation Rings and Base Change

Chandrashekhar Khare

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400 005, India
E-mail: shekhar@math.tifr.res.in

Communicated by K. A. Ribet

Received February 4, 1999

INTRODUCTION AND SUMMARY

Consider a representation $\rho : \Gamma_{\mathbb{Q}} \to GL_n(\mathbb{F})$ where $\Gamma_{\mathbb{Q}}$ is the absolute Galois group of $\mathbb{Q}$, and $\mathbb{F}$ is a finite field of characteristic p. We assume that ρ is absolutely irreducible. Fix a finite set of places S of $\mathbb{Q}$. In [M], Mazur constructs the universal deformation $\rho^{univ} : G_{\mathbb{Q},S} \to GL_n(R_{\mathbb{Q},S})$, where $R_{\mathbb{Q},S}$ is the universal deformation ring, associated to the tuple (ρ, S). The ring $R_{\mathbb{Q},S}$ is a local Noetherian $W(\mathbb{F})$ algebra ($W(\mathbb{F})$ is the ring of Witt vectors of $\mathbb{F}$), with residue field $\mathbb{F}$, and ρ^{univ} is such that modulo the maximal ideal of $R_{\mathbb{Q},S}$, it gives the representation ρ. It is characterised by the universal property that for any local Noetherian ring A with residue field $\mathbb{F}$, any deformation of ρ to $GL_n(A)$, arises from a unique local ring homomorphism $R_{\mathbb{Q},S} \to A$ which induces the identity on residue fields. We refer to [M] as the authoritative source for all the details.

The properties of $R_{\mathbb{Q},S}$ as yet remain mysterious. The only cases when there is a handle on the structure of $R_{\mathbb{Q},S}$ is either when the deformation problem is unobstructed (i.e., $H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\rho)) = 0$), in which case it is a free power series ring on $\dim_{\mathbb{F}} H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\rho))$ generators over the Witt vectors of $\mathbb{F}$, or when $n = 2$ and ρ is a modular representation (following the work of Wiles).

But one may ask if some "relative information" can be obtained. For example one can enlarge the set S to S' and study the resulting map $R_{\mathbb{Q},S'} \to R_{\mathbb{Q},S}$. This has been studied in [B] in many cases. The other case in which there will be a map between "different" deformation rings arises when we restrict ρ to $G_{F,S}$ where F is a number field and S, by abuse of notation, denotes the places of F above those in S. We assume that $F/\mathbb{Q}$ is unramified outside S. We can form the versal deformation ring $R_{F,S}$ and we obtain a map $R_{F,S} \to R_{\mathbb{Q},S}$ (see the next section for more details). It is

0022-314X/99 $30.00

this map, which we will call the base change map, that we propose to study.

We begin with some basic, easy results in the case when the degree of F over $\mathbb{Q}$ is prime to p. We also present various complements, and study the base change map from the point of view of generators and relations. In our earlier paper [K] we showed the relevance of "base change" to the question of lifting 2-dimensional mod p Galois representations to characteristic 0. We go on to point out how the results of [K] may be seen from the perspective of deformation rings. This paper may indeed be viewed as a sequel to [K].

To end, we would like to point out that in a beautiful, recent preprint Ravi Ramakrishna (cf. [R]) has proven that under certain technical conditions 2-dimensional mod p representations of $G_{\mathbb{Q}}$ lift to representations over Witt vectors; the methods of [R] are number theoretical, using the method of auxiliary primes, Tate duality theorems, etc. In contrast, the methods of both [K] and the present paper are cohomological and have nothing to do with number fields.

THE BASE CHANGE MAP: BASICS

The first order of business is to explain how the map $R_{F,S} \to R_{\mathbb{Q},S}$ comes about. As we shall fix S in this section, we deem it fit to drop it as subscripts for the deformation rings below: thus, for instance, the ring $R_{F,S}$ (resp., $R_{\mathbb{Q},S}$) will be denoted just by R_F (resp., $R_{\mathbb{Q}}$).

As recalled above, we have the representation $\rho^{univ}: G_{\mathbb{Q},S} \to GL_2(R_{\mathbb{Q}})$ associated to ρ, and also the representation $\rho_F^{versal}: G_{F,S} \to GL_2(R_F)$ which is the versal deformation associated to ρ restricted to $G_{F,S}$. We may, on the other hand, also restrict ρ^{univ} to $G_{F,S}$, to get $\rho^{univ}|_{G_{F,S}}: G_{F,S} \to GL_2(R_{\mathbb{Q}})$ which we will denote by $\rho^{univ,F}$. The versal property of R_F implies that there exists a local ring homomorphism $\phi: R_F \to R_{\mathbb{Q}}$, such that $\rho^{univ,F} = \phi.\rho_F^{versal}$, which is the *base change* map that we are after. We denote the maximal ideals of R_F and $R_{\mathbb{Q}}$ by $\mathfrak{m}_F$ and $\mathfrak{m}_{\mathbb{Q}}$, respectively.

We now study the map ϕ, assuming that the degree of F over $\mathbb{Q}$ is prime to p. The interest of this special case will become apparent in the next section.

LEMMA 1. *The map $\phi: R_F \to R_{\mathbb{Q}}$ is surjective, assuming that the degree of F over $\mathbb{Q}$ is prime to p.*

Proof. This will follow from Nakayama's lemma provided we succeed in showing that the induced map on the mod p tangent spaces $\mathfrak{m}_F/{\mathfrak{m}_F}^2 + (p) \to \mathfrak{m}_{\mathbb{Q}}/{\mathfrak{m}_{\mathbb{Q}}}^2 + (p)$ is surjective. But the source and target are identified

with the duals of $H^1(G_{F,S}, \mathrm{Ad}(\rho_F))$ and $H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\rho))$ respectively, and the induced map is the dual of the restriction map. As the degree of F over $\mathbb{Q}$ is assumed to be prime to p, the restriction map is injective; one way of seeing this is to observe that the composition *res.cores* is multiplication by $[F:\mathbb{Q}]$. This proves the lemma.

Note. As the referee has remarked there are many possible hypotheses, besides $[F:\mathbb{Q}]$ being prime to p, that imply the conclusion of the above lemma. For instance in the case $n=2$, $p \geqslant 5$, if we assume that the image of ρ is $GL_2(\mathbb{F})$, that the extension $F/\mathbb{Q}$ is linearly disjoint from that cut out by ρ, and that $F/\mathbb{Q}$ has no non-trivial abelian subextensions, then from the vanishing of $H^1(GL_2(\mathbb{F}), \mathrm{Ad}(\rho))$ (see Lemma 1.2 of [Fl] for a proof) one can deduce the injectivity of the restriction map on the corresponding H^1's, implying in turn the surjectivity of the map in the lemma. It may also be possible to impose other hypotheses on $F/\mathbb{Q}$, besides $[F:\mathbb{Q}]$ being prime to p, that imply injectivity of the restriction map $H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\rho)) \to H^2(G_{F,S}, \mathrm{Ad}(\rho))$, that is used to prove Proposition 2 below.

Denote the kernel of the surjective map $\phi : R_F \to R_{\mathbb{Q}}$ by I. Then we have the following proposition.

PROPOSITION 2. *The exact sequence*

$$0 \to I/I^2 \to R_F/I^2 \to R_{\mathbb{Q}} \to 0 \qquad (*)$$

is split, i.e., there exists a local ring homomorphism $\psi : R_{\mathbb{Q}} \to R_F/I^2$, such that $\phi.\psi$ is the identity.

Note. Note that we are abusing notation further by denoting the map $R_F/I^2 \to R_{\mathbb{Q}}$ induced by ϕ by the same symbol.

Proof. The exact sequence $(*)$ yields the exact sequence

$$0 \to M_2(I/I^2) \to GL_2(R_F/I^2) \to GL_2(R_{\mathbb{Q}}) \to 0 \qquad (**)$$

by applying the GL_2 functor. Here $M_2(I/I^2)$ is the additive group of 2 by 2 matrices with coefficients in I/I^2, and is thus abelian. The representation $\rho^{univ} : G_{\mathbb{Q},S} \to GL_2(R_{\mathbb{Q}})$ lifts to a representation with values in $GL_2(R_F/I^2)$ if and only if a certain element γ in $H^2(G_{\mathbb{Q},S}, M_2(I/I^2))$ vanishes, where $G_{\mathbb{Q},S}$ is considered to act on $M_2(I/I^2)$ via the exact sequence $(**)$. This is a basic fact of group cohomology. To be specific we recall that γ is the cohomology class of the cocycle α which is defined by $\alpha(g_1, g_2) = t(g_1 g_2)\, t(g_2)^{-1}\, t(g_1)^{-1}$ where $t(g_1)$, $t(g_2)$, $t(g_1 g_2)$ are elements of $GL_2(R_F/I^2)$, and are arbitrary set theoretic liftings of $\rho^{univ}(g_1)$, $\rho^{univ}(g_2)$, $\rho^{univ}(g_1 g_2)$, respectively.

We claim that the restriction of γ to $G_{F,S}$ vanishes. Note that we have at our disposal the representation $\rho_F^{versal}: G_{F,S} \to GL_2(R_F)$ such that $\phi.\rho^{versal} = \rho^{univ,F}$. Reducing ρ_F^{versal} mod I^2, we get a representation that lifts $\rho^{univ,F} := \rho^{univ}|_{G_F}: G_F \to GL_2(R_{\mathbb{Q}})$. This implies that $\gamma|_{G_F} = 0$, justifying the claim. This implies, as the index of $G_{F,S}$ in $G_{\mathbb{Q},S}$ is prime to p, that γ itself vanishes, and thus by the property of γ noted above, that ρ^{univ} lifts to a representation $\tilde{\rho}^{univ}: G_{\mathbb{Q},S} \to GL_2(R_F/I^2)$. By the versal property of $R_{\mathbb{Q}}$, we get a map $\psi: R_{\mathbb{Q}} \to R_F/I^2$, such that $\tilde{\rho}^{univ} = \psi.\rho^{univ}$ (in fact ψ is then forced to be unique by the universality of $R_{\mathbb{Q}}$). But from the exact sequence $(**)$ we see that $\phi.\psi.\rho^{univ} = \rho^{univ}$. Thus we see by the universal property of $R_{\mathbb{Q}}$ that the composition $\phi.\psi$ is the identity map, which finishes the proof of the proposition.

Remark 3. As the reader can see at a glance, the above proof is cohomological, and it is not of relevance that we are considering representations of Galois groups of number fields.

We would now like to study the base change map $R_F \to R_{\mathbb{Q}}$, (or its mod p reduction) again under the assumption that the degree of F over $\mathbb{Q}$ is prime to p, with relation to the standard way of presenting deformation rings (i.e., by generators "coming from H^1," and relations "from H^2"). This adds a useful perspective on the problem. Our study is motivated by the question:

QUESTION 4. *Does the map* $\phi: R_F \to R_{\mathbb{Q}}$ *split*?

(Or its mod p version: Does the map $\phi: R_F/(p) \to R_{\mathbb{Q}}/(p)$ split?).

Proposition 2 may be viewed as an infinitesimal piece of evidence towards an affirmative answer to this question: it provides the infinitesimal splitting $R_{\mathbb{Q}} \to R_F/I^2$, with the notation above. Our cohomological method does not seem to yield a splitting at even the next stage, namely of the map $R_F/I^3 \to R_{\mathbb{Q}}$.

We must confess, though, that aside from this and the proposition below, we have neither heuristic nor philosophical reasons to hope that the answer is in the positive.

Note. In fact Deligne, in a letter to the author, has pointed out by means of an example that one cannot expect an affirmative answer to Question 4, at least using only generalities of a deformation theory with a trace map available. Note that in the proof of Proposition 2 we only needed to use properties of the restriction and trace (i.e., corestriction) maps in cohomology. We sketch his example: Let $X = \mathrm{Spec}(\mathbb{C}[x,t]/(x^2 - t^2))$ and $T = \mathrm{Spec}(\mathbb{C}[t])$, and consider the quotient map $X \to T$ resulting from the $\mathbb{Z}/2$ action $x \to -x$ on X. We consider the two deformation problems associated to the two functors:

(1) Associate to a noetherian scheme S (over $\mathbb{C}$), morphisms to T with a lifting to X that is fixed by $\mathbb{Z}/2$

(2) Associate to a noetherian scheme S (over $\mathbb{C}$), morphisms to T.

These functors are representable and, by the same reasoning as in the proof of Proposition 2, one does have an infinitesimal splitting of the resulting map of the corresponding universal deformation rings (explicitly, over $t^2=0$, we have a splitting associated to $x \to 0$, $t \to \varepsilon$ with $\mathbb{C}[\varepsilon]$ the dual numbers); but it can be seen that there is no global retraction of the universal deformation rings.

We nevertheless now provide the other small piece of evidence in favour of an affirmative answer to the above question, that uses the more particular features that we have in the setting of deformations of Galois representations:

PROPOSITION 5. *Let F be a finite Galois extension of a number field K of degree prime to p, S a finite set of places of K, including all the infinite places and the places above p. Assume that F/K is unramified outside S, and denote by S the places of F above the places in K. Let $\chi : G_{K,S} \to \mathbb{F}^*$ be a character. Let R_F and R_K be the deformation rings for χ (resp., $\chi|_{G_F}$) with respect to the ramification data S (resp. places of F above S, that we are denoting again by S). Then the map of the associated deformation rings $R_F \to R_K$ splits.*

Proof. This follows from the observation that R_F (resp., R_K) is isomorphic to the completed group algebra of the Galois group of the maximal abelian pro-p extension of F (resp., K) unramified outside S. We indicate the argument. Let K_S (resp., F_S) be the maximal pro-p abelian extension of K (resp. F) unramified outside S and denote the Galois group $\mathrm{Gal}(K_S/K)$ (resp., $G(F_S/F)$) by H (resp., G). Then the extension K_S/K is linearly disjoint from the extension F/K, as $[F:K]$ is prime to p. Thus we have a surjective homomorphism $G \to H$, that is continuous and open with respect to the profinite topology of both the groups. This in turn induces a map of completed group algebras $W(\mathbb{F})[[G]] \to W(\mathbb{F})[[H]]$. The extension F_S/K is Galois, as F/K is Galois; denote its Galois group by G'. The map $G' \to \mathrm{Gal}(F/K)$ is split. Consider the commutant in G (which is a normal subgroup of G') of a lifting of $\mathrm{Gal}(F/K)$ and denote it by H'; $W(\mathbb{F})[[H']]$ is mapped isomorphically to $W(\mathbb{F})[[H]]$ under the map $W(\mathbb{F})[[G]] \to W(\mathbb{F})[[H]]$. This proves the proposition.

Generators and Relations

We choose a presentation of $R_F/(p)$ and $R_{\mathbb{Q}}/(p)$ in the following manner. Let s be the dimension of $H^1(G_{F,S}, \mathrm{Ad}(\rho_F))$ as a $\mathbb{F}$-vector space. Then we can choose a surjective map from $\Sigma_s = \mathbb{F}[[X_1, ..., X_s]]$ to $R_F/(p)$

which induces an isomorphism on the mod p tangent spaces. Denote the kernel by J. The composition of this map with ϕ gives a presentation of $R_{\mathbb{Q}}/(p)$ (though this map may no longer induce an isomorphism on tangent spaces), with kernel say J'. Let $\mathfrak{m}$ denote the maximal ideal of Σ_s. Then we have the exact sequences

$$0 \to J/\mathfrak{m}J \to \Sigma_s/\mathfrak{m}J \to R_F/(p) \to 0$$

$$0 \to J'/\mathfrak{m}J' \to \Sigma_s/\mathfrak{m}J' \to R_{\mathbb{Q}}/(p) \to 0.$$

By the proof of Proposition 2 in [M], we get maps

$$\mathrm{Hom}(J/\mathfrak{m}J, \mathbb{F}) \to H^2(G_{F,S}, \mathrm{Ad}(\rho_F)) \tag{1}$$

and

$$\mathrm{Hom}(J'/\mathfrak{m}J', \mathbb{F}) \to H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\rho)). \tag{2}$$

The first of these maps, (1), is injective by loc. cit.

We have the following proposition.

PROPOSITION 6. *The kernel of* (2) *above is identified with the kernel of the natural map* $(J'/\mathfrak{m}J')^* \to (J/\mathfrak{m}J)^*$.

Proof. This follows from the fact that the restriction map $H^2(G_{\mathbb{Q},S}, \mathrm{Ad}(\rho)) \to H^2(G_{F,S}, \mathrm{Ad}(\rho_F))$ is injective, the commutativity of the diagram obtained by filling in (1) and (2) with the map in the proposition and the restriction map, and the above quoted facts.

Remark 7. (1) One may choose a more economical presentation on $R_{\mathbb{Q}}/(p)$, i.e., inducing isomorphism on mod p tangent spaces. It will be of interest to compare these two presentations, the one via R_F and the one inducing an isomorphism on tangent spaces, in studying the above question.

(2) We will see in the next section that if S is assumed to be sufficiently large we have a map $R_{\mathbb{Q}} \to W_2(\mathbb{F})$ (and *a fortiori* a map $R_F \to W_2(\mathbb{F})$). This is sufficient to ensure (see proof of Proposition 14 below) that we can choose a surjective map $W(\mathbb{F})[[X_1, ..., X_s]] \to R_F$, that induces an isomorphism on tangent spaces. Thus assuming that S is sufficiently large, we could have worked with $R_{\mathbb{Q}}$ and R_F rather that $R_{\mathbb{Q}}/(p)$ and $R_F/(p)$ above.

Remark 8. Assume that F over $\mathbb{Q}$ is Galois with cyclic Galois group Δ of order prime to p. Then R_F has the natural action of Δ and it is known that $R_{\mathbb{Q}}$ is the maximal Δ invariant quotient of R_F (cf. [H]). In this situation, by an easy argument, one may see that there is a $W(\mathbb{F})$-subalgebra of R_F, say R^{Δ}, on which Δ acts trivially, and whose tangent space has the same dimension as that of $R_{\mathbb{Q}}$, and which further maps surjectively to $R_{\mathbb{Q}}$.

Further R^A may be chosen so that the mod I^2 splitting has image in R^A. It can also be checked that R^A has a complement ideal which is mapped to 0 by the base change map. If all this information can be used to produce a splitting is still not clear.

LIFTINGS

The results of the previous section can be used to put the results of [K] in a slightly different perspective.

We write down a result which was noted as a remark in [K].

PROPOSITION 9. *The class γ of the extension*

$$0 \to M_2(\mathbb{F}) \to GL_2(W_2(\mathbb{F})) \to GL_2(\mathbb{F}) \to 0$$

in $H^2(GL_2(\mathbb{F}), M_2(\mathbb{F}))$ is a negligible class.

Note. Here $W_2(\mathbb{F})$ is the Witt vectors of length 2 of $\mathbb{F}$. By γ being negligible, we mean that for any field k and any homomorphism $\tau : G_k \to GL_2(\mathbb{F})$ (where G_k is the absolute Galois group of the separable closure k_s of k), the pullback $\tau^*(\gamma)$ is trivial.

Proof. With notation as above, we must show that $\tau^*(\gamma)$ is 0. In the case when the characteristic of k is not equal to p, this follows directly from the proofs of the Proposition and Theorem 1 in [K]. When the characteristic is p, in the proof of the Proposition in [K], we have to make use of Artin–Schreier extensions (cf., [J, Sect. 8.11]), rather than Kummer extensions; we omit the details.

We transcribe the above result into the setting of deformation rings. Thus we consider an absolutely irreducible representation $\rho : G_{\mathbb{Q}, S} \to GL_2(\mathbb{F})$. We take for F the fixed field of the p-Sylow subgroup of the image of ρ (we may assume that the restriction of ρ to G_F has image in the unipotent matrices). Then the degree of F over $\mathbb{Q}$ is prime to p. By Kummer theory (see the proposition in [K]), we see that if S is large enough, there exists a map $\alpha : R_F \to GL_2(W_2(\mathbb{F}))$. This map is forced to factor through R_F/I^2 (in fact through $R_F/\mathfrak{m}_F^2$). But then Proposition 2 yields that α induces a map $R_{\mathbb{Q}} \to W_2(\mathbb{F})$, and thus produces a lifting of ρ to Witt vectors of length 2.

Remark 10. It is interesting to remark that the map α above coming from Kummer theory, and which factors through the the ring R_F^{red}, the deformation ring parametrising deformations into upper triangular matrices, will not in general factor through $R_{\mathbb{Q}}$. This follows, for instance, from the fact that if ρ is a representation with full image then any lifting

to $GL_2(W_2(\mathbb{F}))$ also has full image (for $p > 5$). But the magic of cohomolgy still yields a map $R_{\mathbb{Q}} \to W_2(\mathbb{F})$, that is induced by α via the splitting of Proposition 2!

Remark 11. We may ask the question if the class of the extension:

$$0 \to M_n(\mathbb{F}) \to GL_n(W_2(\mathbb{F})) \to GL_n(\mathbb{F}) \to 0$$

is negligible for all positive integers n. For $n = 1$ this is trivially true, while for $n = 2$ we have just proven it. For general n, we haven't a clue. For example, consider the "canonical" extension $K/K^{GL_n(\mathbb{F})}$ with Galois group $\mathrm{Gal}(K/K^{GL_n(\mathbb{F})}) = GL_n(\mathbb{F})$, obtained by taking K to be the function field $K = \mathbb{F}(X_1, ..., X_n)$ (with X_i, $1 \leqslant i \leqslant n$ indeterminates), with the natural action of $GL_n(\mathbb{F})$, and $K^{GL_n(\mathbb{F})}$ to be its fixed field. Does this embed in an extension K'/K such that the above exact sequence maps isomorphically to

$$0 \to \mathrm{Gal}(K'/K) \to \mathrm{Gal}(K'/K^{GL_n(\mathbb{F})}) \to \mathrm{Gal}(K/K^{GL_n(\mathbb{F})}) \to 0?$$

We know this to be true by Proposition 9 for $n = 2$, but even in that case we cannot construct K' explicitly.

Remark 12. The methods of [K] do not allow one to assert the existence of a map $R_{\mathbb{Q}} \to W_2(\mathbb{F})$ without possibly enlarging the ramification set S. Is this a limitation of the method used in [K], or are there examples of $\rho : G_{\mathbb{Q}, S} \to GL_2(\mathbb{F})$ (with S consisting only of primes at which ρ ramifies) such that ρ does not lift to a representation $\tilde{\rho} : G_{\mathbb{Q}, S} \to GL_2(W_2(\mathbb{F}))$? Serre's conjectures for odd irreducible ρ only predict the existence of a lift to $\mathcal{O}/\mathfrak{m}^2$ where $\mathcal{O}$ is the ring of integers of a (possibly) ramified extension of $\mathbb{Q}_p$. But note that if $\mathcal{O}$ is the ring of integers of a ramified extension of $W(\mathbb{F})$, then the ring homomorphism $\mathcal{O}/\mathfrak{m}^2 \to \mathbb{F}$ splits. Thus there always exists a *trivial* lift to $\mathcal{O}/\mathfrak{m}^2$ (we are thankful to G. Boeckle for this remark); as once a lift exists the isomorphism class of lifts are parametrised by elements of $H^1(G_{\mathbb{Q}, S}, M_2(\mathbb{F}))$, there are many lifts.

Remark 13. In fact, as is shown in [K], Kummer theory yields a map $R_F \to W(\mathbb{F})$ (which again factors through R_F^{red}), with $W(\mathbb{F})$ the ring of Witt vectors of $\mathbb{F}$. Therefore if the map $R_F \to R_{\mathbb{Q}}$ were to itself split (as asked in Question 4), that would yield the existence of p-adic liftings of 2-dimensional mod p representations.

We note another consequence the existence of the map $R_{\mathbb{Q}} \to W_2(\mathbb{F})$ has. Here, and in the proposition below, the finite set of prime S, that we have suppressed in the notation, is assumed to be large enough for the map $R_{\mathbb{Q}} \to W_2(\mathbb{F})$ to exist. Under this assumption we have:

PROPOSITION 14. *If the Krull dimension of $R_{\mathbb{Q}}/(p)$ is h^1-h^2, then p is not a zero divisor of $R_{\mathbb{Q}}$.*

Remark 15. Here h^i is the dimension of $H^i(G_{\mathbb{Q},S}, \mathrm{Ad}(\rho))$ as a $\mathbb{F}$ vector space. In [M] it is conjectured that the dimension of $R_{\mathbb{Q}}/(p)$ is always h^1-h^2.

Proof. We show that, under the hypotheses of the proposition, the Krull dimension of $R_{\mathbb{Q}}$ is greater that that of $R_{\mathbb{Q}}/(p)$.

We first claim that there exists a surjective map $\alpha : \Sigma := W(\mathbb{F})[[X_1, ..., X_{h^1}]] \to R_{\mathbb{Q}}$ of $W(\mathbb{F})$-algebras that induces an isomorphism on Zariski tangent spaces. The claim follows from the existence of the map $R_{\mathbb{Q}} \to W_2(\mathbb{F})$ as we show below.

Denote by $\mathfrak{m}$ and $\mathfrak{m}_{\mathbb{Q}}$ the maximal ideals of Σ and $R_{\mathbb{Q}}$ respectively. Note that the dimension of $\mathfrak{m}_{\mathbb{Q}}/\mathfrak{m}_{\mathbb{Q}}^2+(p)$ as a $\mathbb{F}$-vector space is h^1. Choose a basis $x_1, ..., x_{h^1}$ of the $\mathbb{F}$-vector space $\mathfrak{m}_{\mathbb{Q}}/\mathfrak{m}_{\mathbb{Q}}^2+(p)$. The existence of the map $R_{\mathbb{Q}} \to W_2(\mathbb{F})$ implies that $p \notin \mathfrak{m}_{\mathbb{Q}}^2$. Thus a basis of the Zariski tangent space $\mathfrak{m}_{\mathbb{Q}}/\mathfrak{m}_{\mathbb{Q}}^2$ of $R_{\mathbb{Q}}$ is $\bar{p}, x_1, ..., x_{h^1}$, where $\bar{p}$ denotes the image of p in $\mathfrak{m}_{\mathbb{Q}}/\mathfrak{m}_{\mathbb{Q}}^2$. Define α by sending X_i to any lift of x_i in $R_{\mathbb{Q}}$; α is surjective by an application of Nakayama's lemma. Then as $\bar{p}, \overline{X_1}, ..., \overline{X_{h^1}}$ is a basis of the $\mathbb{F}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ (where the bar denotes the image in the latter), α induces an isomorphism of the Zariski tangent spaces; this justifies the claim.

Now the proof of the proposition proceeds along the standard lines; we argue just as in the proof of Proposition 2 of [M], that we have used before (cf. the discussion before Proposition 6). Let J be the kernel of α. Consider the exact sequence

$$0 \to J/\mathfrak{m}J \to \Sigma/\mathfrak{m}J \to R_{\mathbb{Q}} \to 0.$$

From this we can define an obstruction class $\mathcal{O}(\rho) \in H^2(G_{\mathbb{Q},S}, M_2(\mathbb{F})) \otimes J/\mathfrak{m}J$ that measures lifting $\rho^{univ} : G_{\mathbb{Q},S} \to GL_2(R_{\mathbb{Q}})$ to $GL_2(\Sigma/\mathfrak{m}J)$. The map $f \to 1 \otimes f(\mathcal{O}(\rho))$ from $\mathrm{Hom}(J/\mathfrak{m}J, \mathbb{F})$ to $H^2(G_{\mathbb{Q},S}, M_2(\mathbb{F}))$ is proved to be injective exactly as in the proof of Proposition 2 of [M], the main point being that α is so chosen as to induce an isomorphism on tangent spaces. This shows that the Krull dimension of $R_{\mathbb{Q}}$ is $\geqslant (h^1+1)-h^2$, h^1+1 being the Krull dimension of Σ. As we are assuming in the proposition that the Krull dimension of $R_{\mathbb{Q}}/(p)$ is h^1-h^2, this finishes the proof.

ACKNOWLEDGMENTS

I gratefully acknowledge the hospitality of Universté de Paris XIII and the financial support of CEFIPRA that I received during work on this paper. I also thank G. Boeckle for helpful conversations, and the referee for an attentive reading of the manuscript.

REFERENCES

[B] N. Boston, Families of Galois representations-increasing the ramification, *Duke Math. J.* **66**, No. 3 (1992), 357–367.

[H] H. Hida, On the Selmer groups of adjoint modular Galois representations, *in* "Number Theory (Paris, 1993–1994)," London Math. Soc. Lecture Note Ser., Vol. 235, pp. 89–128, Cambridge Univ. Press, Cambridge, 1996.

[J] N. Jacobson, "Basic Algebra," Vol. II, Freeman, New York, 1980.

[K] C. Khare, Base change, lifting and Serre's conjecture, *J. Number Theory* **63** (1997), 387–394.

[Fl] M. Flach, A finiteness theorem for the symmetric square of an elliptic curve, *Invent. Math.* **109** (1992), 307–327.

[M] B. Mazur, Deforming Galois representations, *in* "Galois Groups over $\mathbb{Q}$," Math. Sci. Res. Inst. Pub., Vol. 16, pp. 385–437, Springer-Verlag, New York, 1989.

[R] R. Ramakrishna, Lifting Galois representations, preprint.